

Symantec™ Event Collector for Check Point VPN-1/FireWall-1

Integration Guide

Supported Platforms:

Microsoft Windows 2000



Symantec Event Collector for Check Point VPN-1/FireWall-1 Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

Copyright notice

Copyright © 1998–2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then select Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC CORPORATION SOFTWARE LICENSE AGREEMENT COLLECTORS

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

- A. use that number of copies of the Software as have been licensed to you by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, you may make one copy of the Software you are authorized to use on a single machine.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;
- C. use each licensed copy of the Software on a single central processing unit; and
- D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

- A. copy the printed documentation which accompanies the Software;
- B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

- E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module;
- F. use the Software to collect data from a type of technology other than when using a Symantec Event Manager product that corresponds to that type of technology (i.e., antivirus, firewall, IDS, etc.);nor
- G. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

6. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 1	Symantec Event Collector for Check Point VPN-1/ FireWall-1	
	About the Symantec Event Collector for Check Point	10
	About Symantec Enterprise Security Architecture	10
	Symantec Event Collector for Check Point components	11
	How the Symantec Event Collector for Check Point works	12
	How the Symantec Event Collector for Check Point retrieves data	14
	How the Symantec Event Collector for Check Point processes data	14
	How firewall events are mapped from Check Point	15
	Events processed by the Symantec Event Collector for Check Point ...	15
	What the Symantec Event Collector for Check Point CD contains	17
Chapter 2	Installing Symantec Event Collector for Check Point VPN-1/FireWall-1	
	About installation	20
	System prerequisites and set up	22
	Before installing	23
	SESA Manager computer prerequisites	23
	Check Point Log Server prerequisites	24
	SESA DataStore	26
	Installing the SESA integration components	26
	Installing Symantec Event Manager for Firewall – SESA integration components	27
	Installing Symantec Event Collector for Check Point – SESA integration components	27
	Installing on the Check Point Log Server	29
	Installing the Java Runtime Environment	29
	Installing the Symantec Event Manager for Firewall and SESA Agent .	30
	Installing Symantec Event Collector for Check Point	33
	Starting and stopping the Symantec Event Collector for Check Point service	34
	Verifying the installation	35

- Troubleshooting the Symantec Event Collector
 - for Check Point installation37
 - Checking the SESA Manager address and port37
 - Determining whether the SESA Agent is receiving
 - Check Point firewall events38
 - Confirming Symantec Event Collector for Check Point operation38
- Uninstalling39
 - Uninstalling the Symantec Event Collector for Check Point39
 - Uninstalling Symantec Event Manager for Firewall40

Chapter 3 Using the Symantec Event Collector for Check Point VPN-1/FireWall-1

- Viewing reports installed for the Symantec Event Collector
 - for Check Point42
- Customizing firewall event reports43
- Configuring Check Point for Symantec Event Collector
 - for Check Point logging44
- Customizing the SESA Agent configuration45

Index

Symantec Event Collector for Check Point VPN-1/ FireWall-1

This chapter includes the following topics:

- [About the Symantec Event Collector for Check Point](#)
- [Symantec Event Collector for Check Point components](#)
- [How the Symantec Event Collector for Check Point retrieves data](#)
- [What the Symantec Event Collector for Check Point CD contains](#)

About the Symantec Event Collector for Check Point

Symantec Event Collector for Check Point VPN-1/FireWall-1 provides centralized logging, alerting, and reporting for Check Point VPN-1/FireWall-1 Next Generation (NG) products.

Symantec Event Collector for Check Point VPN-1/FireWall-1 retrieves firewall events and forwards these events to the Symantec Enterprise Security Architecture (SESA) management system.

Currently, the logged events represent the operation of the Check Point VPN-1/FireWall-1 NG Feature Pack 2 (FP2) and Feature Pack 3 (FP3) products. These firewall events are stored in the SESA DataStore where they are available for visual inspection, as the basis for alert notifications, and as raw data for report generation.

The Symantec Event Collector for Check Point VPN-1/FireWall-1 requires the Symantec Event Manager for Firewall 1.0 and Symantec Enterprise Architecture Foundation Pack version 1.1.

Note: This guide uses the phrase “Symantec Event Collector for Check Point” to refer to the Symantec Event Collector for Check Point VPN-1/FireWall-1.

About Symantec Enterprise Security Architecture

Symantec Enterprise Security Architecture (SESA) is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide flexible control of security within organizations.

SESA consists of several individual components, that together provide a unique scalable security infrastructure.

Table 1-1 describes these components.

Table 1-1 SESA components

SESA Component	Description
SESA Manager	The SESA Manager is the hub for the SESA Directory and the SESA DataStore. It is a central processing unit (server) for the Agents, DataStore, Directory, and Console. All SESA data passes through the SESA Manager.
SESA DataStore	This relational database stores all event and alert data generated by SESA and SESA-enabled products, such as the Symantec Event Collector for Check Point.
SESA Directory	Stores the configuration data required to manage SESA-enabled security products and SESA services on the network.
SESA Console	The SESA Console is a Java-based, user-interface that provides the graphical user interface to retrieve events and create configurations. It runs in a Web browser with a secure connection.

Symantec Event Collector for Check Point components

Symantec Event Collector for Check Point VPN-1/FireWall-1 installs shared and product-specific components to send Check Point firewall events to SESA. These components are located on the *Symantec Event Manager for Firewall* and *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD-ROMs.

You install the following components in separate procedures.

- Symantec Event Manager for Firewall – SESA integration components
You install these components on every SESA Manager to which you will forward Check Point events.
They extend SESA functionality to provide the Firewall Event Family of reports.
- Symantec Event Collector for Check Point VPN-1/FireWall-1 – SESA integration components
You install these components on every SESA Manager to which you will forward Check Point events.
They extend SESA functionality to provide the Check Point specific reports.

- Symantec Event Manager for Firewall

You install Symantec Event Manager for Firewall on the Check Point Log Server, which is the machine that receives log files from the Check Point firewalls.

The SESA Agent is included with the Symantec Event Manager for Firewall installation. It handles communications between the Symantec Event Collector for Check Point and the SESA Manager. It passes firewall events from the Check Point Log Server to the SESA Manager and receives configuration data.

Note: The Java Runtime Environment (JRE) must already be installed on the computer on which you install the SESA Agent. If necessary, you can install it from the *Symantec Event Manager for Firewall* CD-ROM.

- Symantec Event Collector for Check Point VPN-1/FireWall-1

You install the Symantec Event Collector for Check Point on the Check Point Log Server.

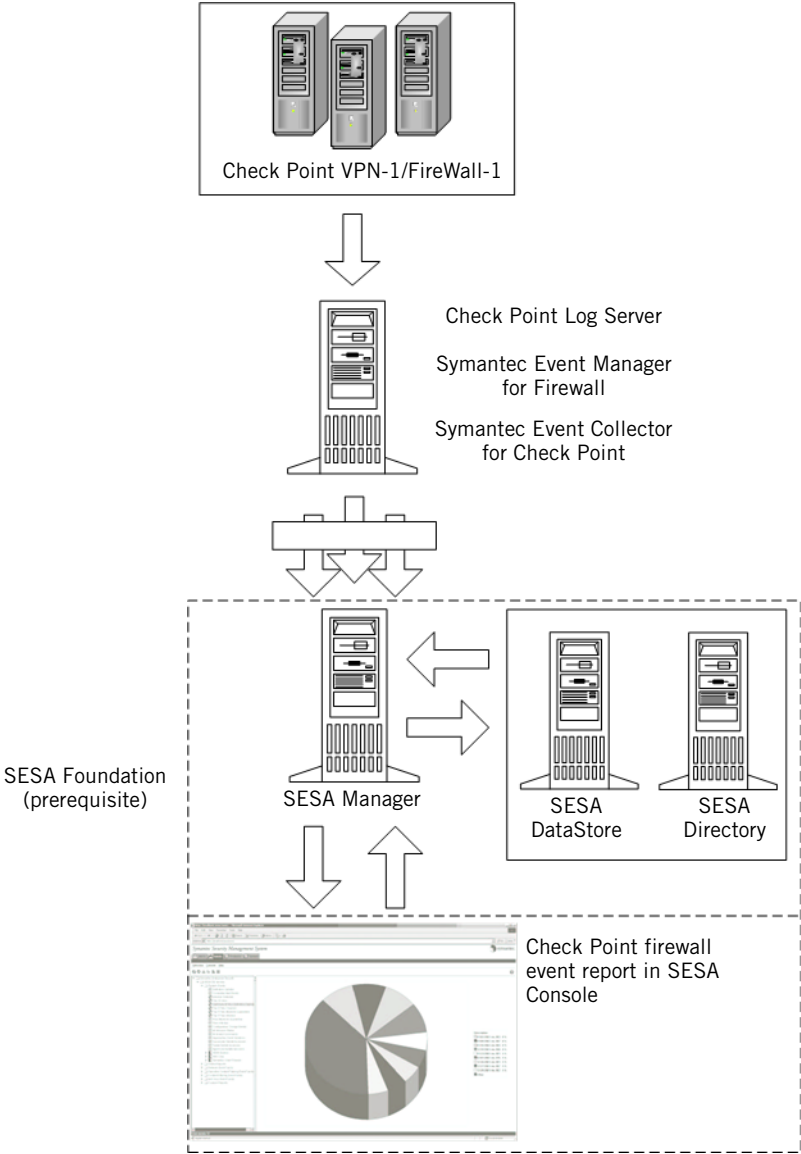
It gathers security event data from Check Point VPN-1/FireWall-1, processes the data into SESA events, and then sends the events to the SESA Manager by way of the SESA Agent.

How the Symantec Event Collector for Check Point works

The Symantec Event Collector for Check Point components work together to collect and route log messages from the Check Point Log Server to SESA. This enables centralized logging, alerting, and reporting using the SESA Console.

[Figure 1-1](#) and the remaining sections of this chapter describe how the Symantec Event Collector for Check Point components collect and route events to the SESA Manager for processing.

Figure 1-1 How the Symantec Event Collector for Check Point collects and sends data to SESA



How the Symantec Event Collector for Check Point retrieves data

The Symantec Event Collector for Check Point VPN-1/FireWall-1 uses two services to forward firewall event information to the SESA Manager: the Symantec Event Collector for Check Point itself, and the SESA Agent.

Both services run on the Check Point Log Server, which is the machine to which your Check Point firewalls forward events. In many cases the Check Point Log Server is also the Check Point Management Server.

The Symantec Event Collector for Check Point waits for new log messages that arrive by way of Check Point's Log Export API (LEA). The LEA enables the Symantec Event Collector for Check Point to receive log data generated by Check Point's VPN-1/FireWall-1 product.

Because the Check Point Log Server can collect log messages from one or many Check Point security gateways, firewall log messages forwarded to SESA by the Symantec Event Collector for Check Point can originate from many end machines.

The SESA Agent securely logs firewall events to a SESA Manager on behalf of the Symantec Event Collector for Check Point. When you install the Symantec Event Manager for Firewall you furnish a small set of initial parameters for the SESA Agent (for example, the SESA Manager's IP address). After you install the SESA Agent, you can change its default parameters using the SESA Console.

How the Symantec Event Collector for Check Point processes data

The Symantec Event Collector for Check Point VPN-1/FireWall-1 is a service that you install on the Check Point Log Server, along with a SESA Agent.

The Symantec Event Collector for Check Point links to the SESA Agent by way of the SESA Agent Application Library (applib). This lets the SESA Agent securely log the firewall events that it receives to a SESA Manager on behalf of the Symantec Event Collector for Check Point.

The Symantec Event Collector for Check Point receives Check Point log messages through Check Point's Log Export API (LEA). The LEA enables the Symantec Event Collector for Check Point to receive real-time log data generated by Check Point VPN-1/FireWall-1.

When product data or the SESA Agent is unavailable, the Symantec Event Collector for Check Point sends error messages to the application event log on the Microsoft Windows system.

When the SESA Manager is unavailable, the SESA Agent queues messages in memory for later delivery, up to a default maximum of 2 MB. Once memory is full, the Agent queues to disk. This queue size can be changed by using the SESA Console to edit the maximum queue size value, as described in [“Customizing the SESA Agent configuration”](#) on page 45.

How firewall events are mapped from Check Point

In the SESA environment, events that arrive from a SESA Agent are generally understood to be events generated by the system on which the SESA Agent is installed.

Because the Symantec Event Collector for Check Point resides on a Check Point Log Server that may receive events from multiple Check Point firewall systems, the event data is structured to uniquely identify each system.

The Symantec Event Collector for Check Point VPN-1/FireWall-1 events are logged as if they originated with the machine that logged the message to the Check Point Log Server.

Events processed by the Symantec Event Collector for Check Point

All SESA events are a discrete instance of a class of similar events. An Event ID field indicates the exact instance. The Symantec Event Collector for Check Point derives discrete event IDs and classifications by examining the contents of key fields.

The Symantec Event Collector for Check Point assigns one of the following categories to each firewall event.

Table 1-2 Symantec Event Collector for Check Point log message categories

Category	Description
Security	Messages that come from a firewall are assigned to the Security category. These can include connection statistic messages.
Application	Events generated by the Symantec Event Collector for Check Point application are listed as Application.

In Check Point, severities are assigned as follows:

Table 1-3 Check Point severities

Severity	Description
Informational	Events that represent expected behavior.
Warning	Events that represent suspicious behavior.

Any Check Point log message can have an “alert” field attached to it, which indicates that the firewall administrator wants extra significance attached to that message. The severity of events created from such log messages is raised to “Warning.” For example, connection messages that are Informational become Warnings when they have an alert field attached.

The combination of the severity determined by the Symantec Event Collector for Check Point and the Check Point assigned severity results in the severity shown in [Table 1-4](#).

Table 1-4 Events processed by the Symantec Event Collector for Check Point

Check Point Event	Category	Severity	Description
Application Start *	Application	Informational	The Symantec Event Collector for Check Point is starting.
Application Stop *	Application	Informational	The Symantec Event Collector for Check Point is stopping.
* These two events are not logged by Check Point. They are generated by the Symantec Event Collector for Check Point. They only indicate that the Symantec Event Collector for Check Point has started or stopped.			
Control Message	Security	Informational or Warning	A “control” log message has been received. These represent various kinds of system-oriented messages.
Key Install	Security	Informational or Warning	A “Key Install” message has been received. A new set of encryption keys has been generated, usually for use by a VPN session.
Connection Accepted	Security	Informational or Warning	A new connection has been accepted.
Connection Dropped	Security	Informational or Warning	A connection attempt was dropped without notifying the source.
Connection Rejected	Security	Informational or Warning	A connection attempt was rejected, actively notifying the source.

Table 1-4 Events processed by the Symantec Event Collector for Check Point

Check Point Event	Category	Severity	Description
Connection Decrypted	Security	Informational or Warning	An incoming VPN connection was accepted.
Connection Encrypted	Security	Informational or Warning	An outgoing VPN connection has been established.
SecurClient User Logon (Authorize)	Security	Informational or Warning	A SecurClient has logged in.
SecurClient User Logoff (De-authorize)	Security	Informational or Warning	A SecurClient has logged off.
SecuRemote User Logon (Authcrypt)	Security	Informational or Warning	A SecuRemote log on has taken place.
User Authentication	Security	Informational or Warning	A user has authenticated.
User Authentication Failure	Security	Warning	A user has failed to authenticate.
Connection Statistics	Security	Informational	<p>A connection has ended. The event fields carry the statistics for the connection.</p> <p>Accounting events carry details regarding the duration of a connection and the amount of data transferred during the connection.</p>

What the Symantec Event Collector for Check Point CD contains

When you install Symantec Event Collector for Check Point you use two CD-ROMs:

- *Symantec Event Manager for Firewall*
- *Symantec Event Collector for Check Point VPN-1/FireWall-1*

The contents of the *Symantec Event Manager for Firewall* CD are described in the *Symantec Event Manager for Firewall Integration Guide*.

Table 1-5 lists the contents of the *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD.

Table 1-5 Symantec Event Collector for Check Point CD contents

CD folder	Contents
top level	<ul style="list-style-type: none">■ cdstart.exe – displays the installation menu to start the Symantec Event Collector for Check Point or SESA integration component installations.■ setup.exe – runs the Symantec Event Collector for Check Point installation. When you insert the CD, a menu option is available to execute setup.exe; it should not be necessary to run setup.exe separately.■ autorun.inf – auto-start program to run cdstart when the CD-ROM is inserted into a Microsoft Windows system.■ Support files for Symantec Event Collector for Check Point installation: Data1.cab, launcher.settings, JREGENT.dll, JWINUTIL.dll, Symantec Event Collector for Check Point VPN-1FireWall-1.msi, libjsunutil.so■ setup.jar – integration component installer program.
\AgtInst	<ul style="list-style-type: none">■ SESA Agent installation files
\techpubs	<ul style="list-style-type: none">■ SEC_CP_RelNote.PDF■ SEC_CP.PDF (<i>Symantec Event Collector for Check Point VPN-1/FireWall-1 Integration Guide</i>)
\lib	<ul style="list-style-type: none">■ Support files for the SESA integration component installation.

Installing Symantec Event Collector for Check Point VPN-1/FireWall-1

This chapter includes the following topics:

- [About installation](#)
- [System prerequisites and set up](#)
- [Before installing](#)
- [Installing the SESA integration components](#)
- [Installing on the Check Point Log Server](#)
- [Starting and stopping the Symantec Event Collector for Check Point service](#)
- [Verifying the installation](#)
- [Troubleshooting the Symantec Event Collector for Check Point installation](#)
- [Uninstalling](#)

About installation

To use the Symantec Event Collector for Check Point VPN-1/FireWall-1, you install components on the following computers:

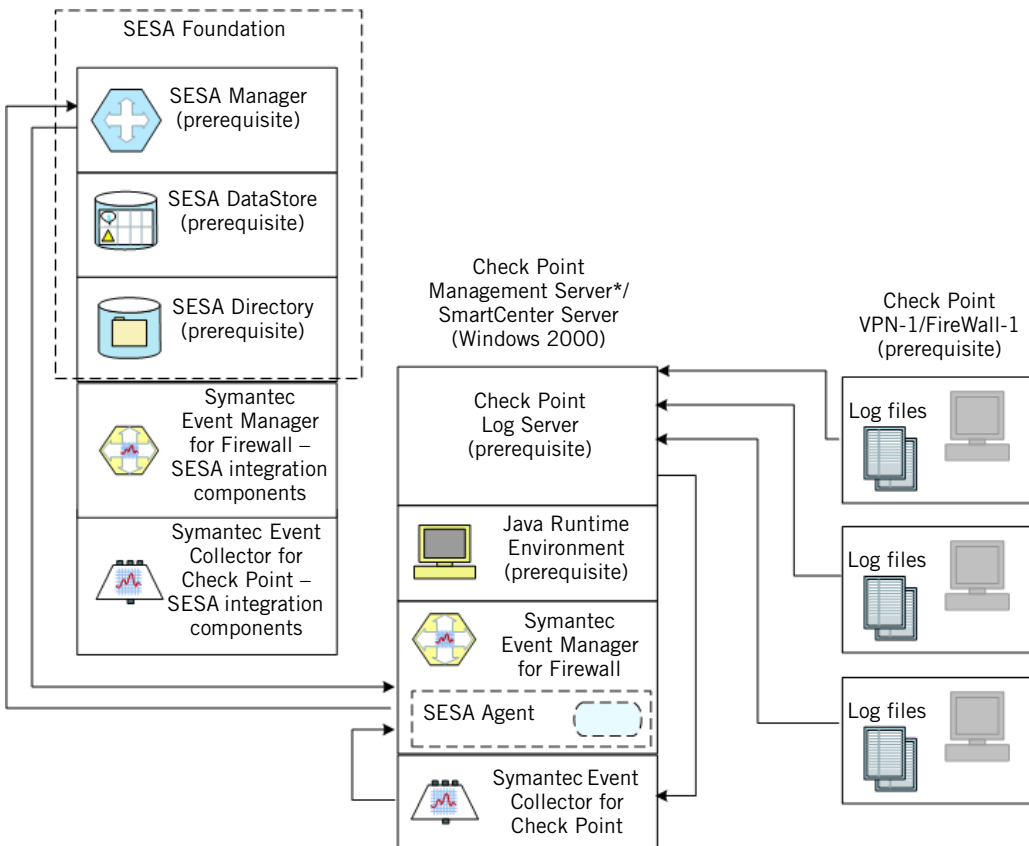
- The SESA Manager to which the Check Point firewall events are forwarded

Note: SESA Foundation Pack 1.1 must be installed on the SESA Manager before you begin installing the Symantec Event Collector for Check Point.

- The Check Point Log Server that collects Check Point VPN-1/FireWall-1 log messages

Figure 2-1 shows the components that you install and where you install them.

Figure 2-1 Symantec Event Collector for Check Point components



* This figure assumes that the Check Point Log Server is installed on the Check Point Management Server.

Complete the installation in the following order:

- 1 Ensure connectivity between the SESA Manager and the Check Point Log Server.
See [“SESA Manager computer prerequisites”](#) on page 23 and [“Check Point Log Server prerequisites”](#) on page 24.
- 2 On the SESA Manager, install the Symantec Event Collector for Check Point SESA integration components.
These extend SESA functionality to use the Symantec Event Collector for Check Point event data by providing the Firewall Event Family reports and Check Point specific reports that let you view and manage Check Point events in SESA.
See [“Installing Symantec Event Manager for Firewall – SESA integration components”](#) on page 27.
See [“Installing Symantec Event Collector for Check Point – SESA integration components”](#) on page 27.
- 3 On the Check Point Log Server (which is usually the Check Point Management Server), install the following components:
 - Java Runtime Environment (JRE) version 1.3.1_02
The JRE is required to install SESA Agent component of the Symantec Event Manager for Firewall.
See [“Installing the Java Runtime Environment”](#) on page 29.
 - Symantec Event Manager for Firewall
The Symantec Event Manager for Firewall includes the SESA Agent that forwards events to the SESA Manager.
See [“Installing the Symantec Event Manager for Firewall and SESA Agent”](#) on page 30.
 - Symantec Event Collector for Check Point VPN-1/FireWall-1
The Symantec Event Collector for Check Point collects events from the Check Point log files and formats them for SESA.
See [“Installing Symantec Event Collector for Check Point”](#) on page 33.

System prerequisites and set up

The system prerequisites for installing the Symantec Event Collector for Check Point are the same as those for installing the Check Point Log Server and the SESA Manager.

Table 2-1 and Table 2-2 list the basic prerequisites.

Table 2-1 Hardware prerequisites

System	Requirements
Check Point Log Server	Intel Pentium class system
SESA Manager	Pentium 800 MHz or higher (1 GHz or higher recommended)

Table 2-2 Software prerequisites

System	Requirements
Check Point Log Server	Microsoft Windows 2000 Check Point VPN-1/FireWall-1 NG Feature Pack 2 or Feature Pack 3 Check Point Log Server component
SESA Manager	Windows 2000 Server/Advanced Server with Service Pack 2 and the latest Microsoft security patches SESA Foundation Pack 1.1

The Check Point Log Server component can be installed on the Check Point management server, or on another computer. For details of the prerequisites for Check Point, see your Check Point documentation

For details of the prerequisites for the SESA Manager, see the *Symantec Enterprise Security Architecture Installation Guide*. Note that the SESA DataStore computer, installed during the installation of the SESA Foundation Pack, must have enough hard disk space to accommodate the additional firewall security events that the Symantec Event Collector for Check Point will send.

The Symantec Event Collector for Check Point also requires the installation of the Symantec Event Manager for Firewall on the Check Point Log Server and on each SESA Manager to which Check Point firewall events will be sent. Installation instructions are provided in this guide and in the *Symantec Event Manager for Firewall Integration Guide*.

Before installing

This section describes the prerequisites that must be met before you begin installing the components of the Symantec Event Collector for Check Point.

The prerequisite software must be installed, as shown in [Figure 2-1](#). You must also ensure that you have connectivity between the SESA Manager and the Check Point Log Server.

SESA Manager computer prerequisites

Before installing any components on the SESA Manager, ensure that it is installed and operating properly. For installation information, see the *Symantec Enterprise Security Architecture Installation Guide*.

Install the SESA integration components for the Symantec Event Collector for Check Point on the SESA Manager before you install the Symantec Event Collector for Check Point on the Check Point Log Server. If you do not install the SESA integration components, you cannot connect the Symantec Event Collector for Check Point to the SESA Manager.

See [“Installing the SESA integration components”](#) on page 26.

Ensuring connectivity from the Log Server to the SESA Manager

By default, the SESA Agent connects to the SESA Manager using HTTPS on port 443. You can configure a different port if desired.

Appropriate routing must exist between the SESA Agent and SESA Manager so that firewall event messages can reach the SESA Manager.

In addition, make sure that there is no firewall policy blocking the connection between the SESA Agent and the SESA Manager.

To test for connectivity

- ◆ At a command prompt issue the following command:
telnet <SESA-IP-address> 443
where <SESA-IP-address> is the IP address of the SESA Manager.
The connection should appear to hang, but not be refused. After typing a few characters, there should be a message that the connection has been lost.

If the connection is refused, make sure that the Check Point firewall has a rule that allows traffic to the SESA Manager. See [“Allowing traffic from the Symantec Event Collector for Check Point to the SESA Manager”](#) on page 24.

Check Point Log Server prerequisites

Symantec Event Manager for Firewall, the SESA Agent, and the Symantec Event Collector for Check Point VPN-1/FireWall-1 must be installed on the computer that is running the Check Point Log Server.

Before you install any components on the Check Point Log Server, ensure that it is installed and operating properly. For installation information, see your Check Point documentation.

Use the Check Point Log Viewer (if you are running FP2) or Check Point SmartView Tracker (if you are running FP3) to verify that the firewalls to be monitored are passing traffic and logging appropriately.

In addition, complete the instructions in the following sections:

- [“Ensuring connectivity from the Log Server to the SESA Manager”](#) on page 23
- [“Allowing traffic from the Symantec Event Collector for Check Point to the SESA Manager”](#) on page 24
- [“Configuring the LEA port for use by the Symantec Event Collector for Check Point”](#) on page 25

Allowing traffic from the Symantec Event Collector for Check Point to the SESA Manager

If you plan to install the Symantec Event Collector for Check Point on a Check Point Log Server on which there is also a firewall, Check Point must be configured to allow traffic from the Symantec Event Collector for Check Point to the SESA Manager.

You can do this with either an implied policy rule that lets all traffic that originates from the firewall computer pass, or by creating an explicit rule. Depending on how your Check Point environment is currently set up, this may or may not require additional action on your part.

To allow traffic from the Symantec Event Collector for Check Point to the SESA Manager

- 1 On the Check Point Log Server, do one of the following:
 - If you are using Check Point VPN-1/FireWall-1 FP2, open the Check Point Policy Editor.
 - If you are using Check Point VPN-1/FireWall-1 FP3, open the Check Point SmartDashboard.

- 2 Do one of the following:
 - Ensure that you have an implied policy rule that lets all traffic that originates from the firewall computer pass.
To do this, display the Global Properties window.
Verify that the Accept outgoing packets originating from gateway check box is checked. By default, this option is enabled.
 - Create an explicit rule that lets traffic pass from the Symantec Event Collector for Check Point to the SESA Manager.
- 3 If you create an explicit rule, ensure that Tracking is set to None for the rule.
To prevent recursive log messages, traffic between the Symantec Event Collector for Check Point and its SESA Manager must not be logged to the Check Point Log Server that the Symantec Event Collector for Check Point is monitoring.
This includes the machine on which the Symantec Event Collector for Check Point is installed, as well as any firewall in the network path to the SESA Manager.
If such traffic were logged, each Check Point log message would cause the Symantec Event Collector for Check Point to log a SESA event, which in turn would cause a Check Point log message.

Configuring the LEA port for use by the Symantec Event Collector for Check Point

You should configure the LEA port so that the Symantec Event Collector for Check Point can access LEA unauthenticated and unencrypted at port 18184. This is the default LEA port, but not the default authentication mechanism.

Configuring the LEA port in this way lets any host connect to the LEA server and read log data.

Create a policy rule to prevent access from any source other than the local machine.

To configure the LEA port for use by the Symantec Event Collector for Check Point

- 1 Navigate to the directory containing the fwopsec.conf file. This file is usually in the following location:
C:\WINNT\FW1\NG\conf\fwopsec.conf
- 2 Open the fwopsec.conf file in the WordPad editor; do not use Notepad.

- 3 Type the following lines into the file:

```
lea_server port 18184
```

```
lea_server auth_port 0
```

This reverses the values for port and auth_port that are in the original file.

- 4 Save fwopsec.conf.
Ignore the “lose format” warning when saving.

SESA DataStore

After you install the Symantec Event Collector for Check Point and the SESA integration components, Check Point can begin to forward firewall events to SESA. The amount of disk space you will need to accommodate the event data depends on how many devices are logging events, how verbose they are, and how long you want to keep the event data.

We recommend a minimum of 128 GB free space to ensure that events are properly logged.

Installing the SESA integration components

You install the Symantec Event Manager for Firewall and Symantec Event Collector for Check Point SESA integration components on the SESA Manager.

You perform two separate installation procedures:

- Use the *Symantec Event Manager for Firewall* CD-ROM to install the Symantec Event Manager for Firewall – SESA integration components.
- Use the *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD-ROM to install the Symantec Event Collector for Check Point – SESA integration components.

These components must be installed before you install the Symantec Event Manager for Firewall and the Symantec Event Collector for Check Point on the Check Point Log Server. This is required so that after you install on the Check Point Log Server, you can connect to SESA.

You must install both sets of components on every SESA Manager to which you will forward Check Point events.

Installing Symantec Event Manager for Firewall – SESA integration components

You must install the Symantec Event Manager for Firewall – SESA integration components before you install the Symantec Event Collector for Check Point – SESA integration components.

These components contain the Firewall Event Family common reports and the Symantec Security Gateway reports.

Use the *Symantec Event Manager for Firewall* CD-ROM to perform the installation on every SESA Manager to which you are forwarding Check Point firewall events.

For installation instructions, see the section on installing Symantec Event Manager for Firewall – SESA integration components in the *Symantec Event Manager for Firewall Integration Guide*.

Installing Symantec Event Collector for Check Point – SESA integration components

You install the Symantec Event Collector for Check Point – SESA integration components to provide reports that are specific to Check Point VPN-1/Firewall-1.

You must install these components on every SESA Manager to which you are forwarding Check Point firewall events.

To install Symantec Event Collector for Check Point – SESA integration components

- 1 On the SESA Manager computer, insert the *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD.
 If the installation program does not start automatically, navigate to the CD-ROM drive and double-click **cdstart.exe**.
- 2 In the Symantec Enterprise Security Architecture dialog box, click **Install SESA Integration Components**.
- 3 In the Welcome to the SESA Integration Wizard window, click **Next**.
- 4 In the SESA Integration Requirements dialog box, verify that you have the SESA Manager running on this machine, then do one of the following:
 - If you have satisfied these requirements, click **Next**.
 - If you have not satisfied these requirements, click **Cancel**.
 This exits you from setup, so that you can install the necessary files.

5 In the SESA Domain Administrator Information dialog box, do the following:

SESA Domain Administrator Name	Type the name of the SESA Domain Administrator account.
SESA Domain Administrator Password	Type the password for the SESA Domain Administrator account.
IP Address of SESA Directory	Type the IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you use authenticated SSL instead of the SESA default, anonymous SSL, you must type the host name of the SESA Directory computer. For example, myhost.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the <i>Symantec Enterprise Security Architecture Installation Guide</i> .
SSL Port	Type the number of the SESA Directory secure port. By default, the port number is 636.

6 Click **Next**.

7 In the Ready to proceed dialog box, do one of the following:

- If you are ready to proceed, click **Next**.
- If you want to change your settings, click **Back**.

8 In the Configuring Your System dialog box, you will see the progress of the configuration of the SESA Console for the Symantec Event Collector for Check Point VPN-1/FireWall-1. When it is complete, click **Next**.

9 In the SESA Console Integration Status window, verify that your installation was successful, then click **Finish**.

10 Repeat steps 1 through 9 on each SESA Manager to which you will forward Check Point events.

Installing on the Check Point Log Server

You install the products that enable the forwarding of Check Point firewall events to SESA on the Check Point Log Server.

Install the following products in the order in which they are listed:

- Use the *Symantec Event Manager for Firewall* CD-ROM to install
 - Java Runtime Environment (JRE) version 1.3.1_02
 - Symantec Event Manager for Firewall
- Use the *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD-ROM to install Symantec Event Collector for Check Point VPN-1/FireWall-1.

Installing the Java Runtime Environment

The Java Runtime Environment (JRE) version 1.3.1_02 is required by the SESA Agent. If it is not already present on your system, it must be installed before you install the Symantec Event Manager for Firewall, which includes the SESA Agent installation.

To install the Java Runtime Environment

Determine whether the correct version of the JRE is already installed on your Check Point Log Server.

If it is not, perform the JRE installation procedure.

To determine whether the Java Runtime Environment is installed

- 1 On the Check Point Log Server, at the DOS prompt, type the following command:
`java -version`
- 2 Verify that the Java Runtime Environment is installed and that the java version is 1.3.1_02.
- 3 If it is not, install the Java Runtime Environment before you install the Symantec Event Manager for Firewall.

To install the Java Runtime Environment

- 1 On the Check Point Log Server, insert the *Symantec Event Manager for Firewall* CD into the CD-ROM drive.
If the installation program does not start automatically, navigate to the CD-ROM drive and double-click `cdstart.exe`.

- 2 In the Symantec Enterprise Security Architecture dialog box, click **Install JRE 1.3.1_02**.
The Java files are unpacked and the Java installation is launched.
- 3 Complete the installation as prompted.

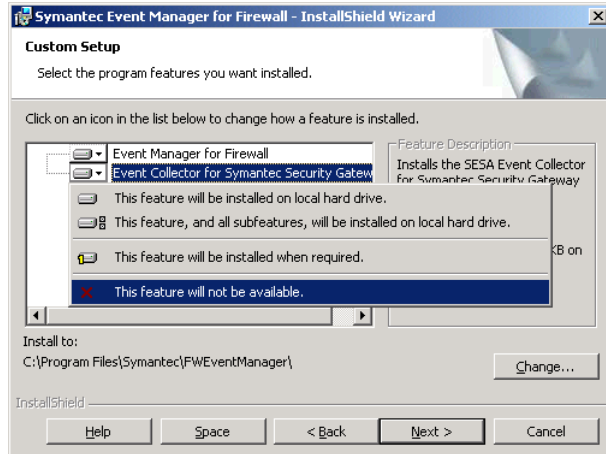
Installing the Symantec Event Manager for Firewall and SESA Agent

Before you install the Symantec Event Collector for Check Point, you must install the Symantec Event Manager for Firewall and SESA Agent.

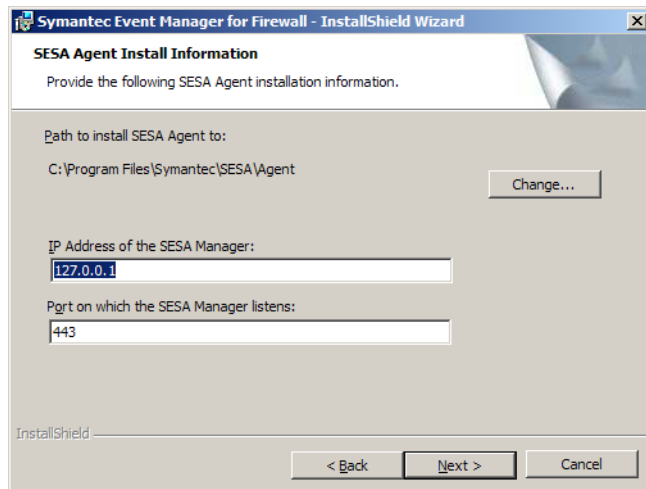
To install the Symantec Event Manager for Firewall

- 1 On the Check Point Log Server, insert the *Symantec Event Manager for Firewall* CD into the CD-ROM drive.
If the installation program does not start automatically, navigate to the CD-ROM drive and double-click **cdstart.exe**.
- 2 In the Symantec Enterprise Security Architecture dialog box, click **Install Event Manager for Firewall**.
- 3 In the Event Manager for Firewall InstallShield Wizard Welcome dialog box, click **Next**.
- 4 In the License Agreement dialog box, read the License Agreement and do one of the following:
 - If you accept the license terms, click **I accept the terms in the license agreement**. Then click **Next**.
 - If you do not accept the license terms, click **I do not accept the terms in the license agreement**.
This cancels the installation process.

- 5 In the Custom Setup dialog box, click the icon beside Event Collector for Symantec Security Gateways.



- 6 In the drop-down list, next to This feature will not be available, click the red X.
- 7 Click Next.
- 8 If a SESA Agent is not already installed on your system, the SESA Agent Install Information dialog box is displayed.
If you do not see this dialog box, proceed to step 11.



9 In the SESA Agent Install Information dialog box, do the following:

- | | |
|---|---|
| Path to install SESA Agent to: | <ul style="list-style-type: none">■ If you accept the default installation location, leave this unchanged.■ If you want to change the location where the SESA Agent is installed, click Change. In the Change the SESA Agent Distribution Folder dialog box, specify the destination folder for the SESA Agent, then click OK. |
| IP Address of the SESA Manager: | <ul style="list-style-type: none">■ If SESA is using default anonymous SSL, type the IP address of the SESA Manager computer.■ If SESA has been upgraded to use authenticated SSL, type the host name of the SESA Manager computer. |
| Port on which the SESA Management Server listens: | Type the port number if it is other than the default, 443. |

10 Click **Next**.

11 In the Ready to Install the Program dialog box, click **Install**.

A DOS window shows the installation of files. When it closes, the Status field of the Installing Event Collector dialog box shows the progress of the installation of the SESA Agent.

12 In the InstallShield Wizard Completed dialog box, click **Finish**.

13 When you are prompted to restart your system, do one of the following:

- To restart now, click **Yes**.
- To restart later, click **No**.

Note: You must restart your system to complete the installation of the SESA Agent; however, you can wait until after you have installed the Symantec Event Collector for Check Point software.

Installing Symantec Event Collector for Check Point

After you install Symantec Event Manager for Firewall, you install Symantec Event Collector for Check Point VPN-1/FireWall-1 on the Check Point Log Server.

The installation process installs the Symantec Event Collector for Check Point as a service. The Symantec Event Collector for Check Point is accessible through the Services control panel applet. It is also accessible through the Add/Remove Programs control panel applet.

To install Symantec Event Collector for Check Point

- 1 On the Check Point Log Server, insert the *Symantec Event Collector for Check Point VPN-1/FireWall-1* CD-ROM into the CD-ROM drive.
If the installation program does not start automatically, navigate to the CD-ROM drive and double-click **cdstart.exe**.
- 2 In the Symantec Enterprise Security Architecture dialog box, click **Install Symantec Event Collector for Check Point FW-1**.
- 3 In the Symantec Event Collector for Check Point VPN-1/FireWall-1 InstallShield Wizard Welcome dialog box, click **Next**.
- 4 In the License Agreement dialog box, read the License Agreement and do one of the following:
 - If you accept the license terms, click **I accept the terms in the license agreement**. Then click **Next**.
 - If you do not accept the license terms, click **I do not accept the terms in the license agreement**.
This cancels the installation process.
- 5 The Custom Setup dialog box shows the default location to which the Symantec Event Collector for Check Point is installed:
C:\Program Files\Symantec\Event Collector for Check Point
Do one of the following:
 - To install the Symantec Event Collector for Check Point to the default location, click **Next**.
 - To change the installation location for the Symantec Event Collector for Check Point, click **Change**.
In the Change Current Destination Folder dialog box, select a new location for the Symantec Event Collector for Check Point, click **OK**, and then click **Next**.

- 6 In the Ready to Install the Program dialog box, click **Install**.
A DOS window shows the installation of the Symantec Event Collector for Check Point files.
- 7 In the InstallShield Wizard Completed dialog box, click **Finish**.
- 8 When you are prompted to restart your system, do one of the following:
 - To restart now, click **Yes**.
 - To restart later, click **No**.You must restart your system before you can use the Symantec Event Collector for Check Point VPN-1/FireWall-1.

Starting and stopping the Symantec Event Collector for Check Point service

The Symantec Event Collector for Check Point runs as a service on the computer on which the it is installed. To start and stop the Symantec Event Collector for Check Point, you start and stop the service as necessary.

You can also stop the Symantec Event Collector for Check Point by stopping the SESA Agent service.

To start or stop a service

- 1 On Check Point Log Server, on the desktop, right click **My Computer** and click **Manage**.
- 2 In the Computer Management window, expand **Services and Applications** and click **Services**.
- 3 In the right pane, select the Symantec Event Collector for Check Point VPN-1/FireWall-1 service.
- 4 On the toolbar, click **Start** or **Stop**.

Verifying the installation

After installation, you can verify that the appropriate components are installed and working properly.

Verify the installation

To verify the installation, do the following:

- Verify that the appropriate services have started.
- Verify that the reports and products you installed for Symantec Event Manager for Firewall and Symantec Event Collector for Check Point are displayed in the SESA Console.
- Examine the Symantec Event Collector for Check Point and SESA Agent logs as necessary.

To verify that the appropriate services have started

- 1 On the Check Point Log Server, select **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 In the Services window, verify that the following services are running:
 - Symantec Event Collector for Check Point VPN-1/FireWall-1
 - SESA AgentStart Service

To verify that the reports and products you installed are displayed in the SESA Console

- 1 On the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.

Note: If you are not working directly on the SESA Manager computer, to connect to the SESA Console, in a browser window type the URL of the SESA Manager.

- 2 Log on to the SESA Console using a SESA user account with sufficient rights to view SESA configurations.
The SESA user must belong to a role that has rights to the SESA-enabled Symantec Event Collector for Check Point VPN-1/FireWall-1 product.
- 3 On the Event view tab, expand your domain, and then expand **SESA DataStore > Firewall Event Family**.
- 4 Under Firewall Event Family, verify that the Symantec Security Gateway folder is listed.

Verifying the installation

- 5 Verify that the Symantec Event Collector for Check Point VPN-1/FireWall-1 folder is listed and contains the following reports:
 - All Check Point events
 - All Check Point alerts (if created in Check Point)
- 6 On the Configurations view tab, expand your domain.
- 7 Verify that the following items are listed:
 - Symantec Security Gateways
 - Symantec Event Collector for Check Point VPN-1/FireWall-1

For more information on reports and views, see the *Symantec Enterprise Security Architecture Administrators Guide*.

To examine the Symantec Event Collector for Check Point and SESA Agent logs

- 1 On the computer on which the Symantec Event Collector for Check Point is installed, navigate to the SESA Agent log.
The default location is:
C:\Program Files\Symantec\SESA\Agent\sesa-agent.log
- 2 Ensure that the log contains the following entry:
SESA Agent ***Bootstrap successful
If you do not see this message, see the procedure [“Checking the SESA Manager address and port”](#) on page 37.
- 3 Select **Start > Settings > Control Panel > Administrative Tools > Event Viewer**.
- 4 Click **Application Log**.
- 5 Examine the log.
The following Symantec Event Collector for Check Point VPN-1/FireWall-1 event should be present:
The service was started

Troubleshooting the Symantec Event Collector for Check Point installation

If you are not receiving Check Point firewall events after you have installed Symantec Event Collector for Check Point VPN-1/FireWall-1 and have run the verification procedures described previously, perform the following procedures to confirm operation:

- [Checking the SESA Manager address and port](#)
- [Determining whether the SESA Agent is receiving Check Point firewall events](#)
- [Confirming Symantec Event Collector for Check Point operation](#)

Checking the SESA Manager address and port

Verify that you specified the correct SESA Manager IP address (or host name) and the correct number for the SESA secure directory port when you ran the Symantec Event Manager for Firewall installation.

To check the SESA Manager address and port

- 1 On Check Point Log Server, at the command prompt, change directories to the following folder on the hard drive:
C:\Program Files\Symantec\SESA\Agent
- 2 In a text editor, open the Configprovider.cfg file.
- 3 Verify that the following options contain the correct settings for the SESA Manager to which you want to send Check Point firewall events:

mgmtServer	IP address of the SESA Manager
mgmtPort	Port that you choose for secure data. Default: 443

If these values are incorrect, you can edit them to provide the correct values. You should not edit these settings if the sesa-agent.log file indicates a successful bootstrap of the SESA Agent. See [“Verifying the installation”](#) on page 35.

Determining whether the SESA Agent is receiving Check Point firewall events

Determine whether the SESA Agent is being updated with firewall events from Check Point.

To determine whether the SESA Agent is receiving Check Point firewall events

- 1 On the Check Point Log Server, at the command prompt, change directories to the following folder on the hard drive:
C:\Program Files\Symantec\SESA\Agent
- 2 Type the following command:
java -jar agentcmd.jar -status
A list is generated, showing the number of events in the SESA Agent queue, and the number of events that have been processed.
In the queues that are displayed, look for “ProdID 3030”, which is the product ID for the Symantec Event Collector for Check Point.

If you do not see ProdID 3030, reinstall the Symantec Event Collector for Check Point VPN-1/FireWall-1 SESA integration components.

Confirming Symantec Event Collector for Check Point operation

You can confirm Symantec Event Collector for Check Point operation by checking that the proper services are running and that there are no error messages in the application log file.

To confirm Symantec Event Collector for Check Point operation

- 1 On the Check Point Log Server, select **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 In the Services window, verify that the following services are running:
 - Symantec Event Collector for Check Point VPN-1/FireWall-1
 - SESA AgentStart ServiceIf these services are not running, uninstall and reinstall the Symantec Event Manager for Firewall and Symantec Event Collector for Check Point VPN-1/FireWall-1.
- 3 Close the Services window.

- 4 Select **Event Viewer**.
- 5 In the Event Viewer, examine the Windows Application Log for failure events from the Symantec Event Collector for Check Point VPN-1/FireWall-1.
If you see only success events, the Symantec Event Collector for Check Point is working properly and the problem probably exists elsewhere.
If you see failure events, contact Symantec support.
- 6 Close the Event Viewer and the Administrative Tools windows.

Uninstalling

If you want to uninstall the Symantec Event Collector for Check Point VPN-1/FireWall-1, you uninstall both the Symantec Event Collector for Check Point software and Symantec Event Manager for Firewall software.

The uninstall process reverses the order of the install process, so that you uninstall the Symantec Event Collector for Check Point first.

Uninstalling the Symantec Event Collector for Check Point

You uninstall the Symantec Event Collector for Check Point using the Microsoft Windows Add/Remove Programs feature.

After you uninstall, the Symantec Event Collector for Check Point VPN-1/FireWall-1 service is removed from the Windows Services window (service control manager).

To uninstall the Symantec Event Collector for Check Point

- 1 On the Check Point Log Server, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs dialog box, click **Symantec Event Collector for Check Point VPN-1/FireWall-1**, then click **Remove**.
- 4 When you are prompted to remove Symantec Event Collector for Check Point VPN-1/FireWall-1 from your computer, click **Yes**.

Symantec Event Collector for Check Point VPN-1/FireWall-1 is removed from the Add/Remove Programs dialog box, indicating that the Symantec Event Collector for Check Point is removed.

Uninstalling Symantec Event Manager for Firewall

You uninstall Symantec Event Manager for Firewall using the Microsoft Windows Add/Remove Programs feature.

Uninstalling Symantec Event Manager for Firewall also removes the SESA Agent if no other products on the Check Point Log Server are using it.

After you uninstall, the SESA AgentStart service is removed from the Windows Services window (service control manager).

To uninstall Symantec Event Manager for Firewall

- 1** On the Check Point Log Server, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2** In the Control Panel window, double-click **Add/Remove Programs**.
- 3** In the Add/Remove Programs dialog box, click **Symantec Event Manager for Firewall**, then click **Remove**.
- 4** When you are prompted to remove Symantec Event Manager for Firewall from your computer, click **Yes**.

Symantec Event Manager for Firewall is removed from the Add/Remove Programs dialog box, indicating that the Event Manager is removed.

Using the Symantec Event Collector for Check Point VPN-1/FireWall-1

This chapter includes the following topics:

- [Viewing reports installed for the Symantec Event Collector for Check Point](#)
- [Customizing firewall event reports](#)
- [Configuring Check Point for Symantec Event Collector for Check Point logging](#)
- [Customizing the SESA Agent configuration](#)

Viewing reports installed for the Symantec Event Collector for Check Point

The Symantec Event Collector for Check Point VPN-1/FireWall-1 lets you use the SESA Console to view firewall events logged by your Check Point firewalls.

The SESA integration components that you installed on the SESA Manager include pre-defined reports for firewall and Check Point collector events.

The Firewall Event Family contains reports that are common to all firewall products. For details of these reports, see the *Symantec Event Manager for Firewall Integration Guide*.

The reports that are specific to firewall events collected for Check Point are found in the Symantec Event Collector for Check Point VPN-1/FireWall-1 folder within the Firewall Event Family.

The following table describes the firewall event reports that are specific to the Symantec Event Collector for Check Point:

Table 3-1 Symantec Event Collector for Check Point VPN-1/FireWall-1 reports

Report name	Report format	Description
All Check Point events	Table	All events logged by Check Point VPN-1/FireWall-1.
All Check Point alerts	Table	Details of Check Point alerts.

To view Symantec Event Collector for Check Point reports

- 1

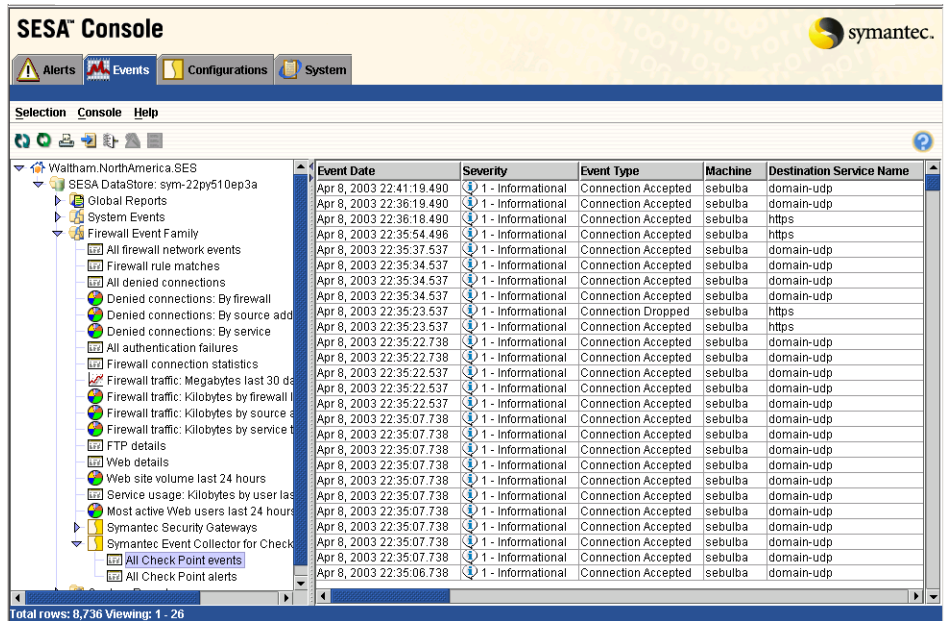
Log on to the SESA Console using a SESA user account with sufficient rights to view SESA events.

The SESA user must belong to a role that has rights to the SESA-enabled security gateway product. See the *Symantec Enterprise Security Architecture Administrator’s Guide* for information on roles.
- 2

On the Events view tab, in the left pane, expand <Domain Name> > SESA DataStore > Firewall Event Family to display all common Firewall Event Family reports.

To display available Symantec Event Collector for Check Point reports, expand <Domain Name> > SESA DataStore > Firewall Event Family> Symantec Event Collector for Check Point VPN-1/FireWall-1.

Click the icon or name of the report you want to view. The report appears in the right pane.



Customizing firewall event reports

In addition to the reports in the Firewall Event Family and the Symantec Event Collector for Check Point VPN-1/FireWall-1 folder, you can create customized event reports that display data that is of interest to your organization.

For example, to create a report that shows all connection attempts for a specific address, you can display the All Firewall Events report and add a filter that focuses the report on the address that you are interested in.

For more information, see the section on creating custom reports in the *Symantec Enterprise Security Architecture Administrators Guide*.

Configuring Check Point for Symantec Event Collector for Check Point logging

No configuration of the Symantec Event Collector for Check Point VPN-1/FireWall-1 is necessary. By default, most events that are logged to the Check Point Log Server are captured by the Symantec Event Collector for Check Point and logged to the SESA Manager.

Use the Check Point Policy Editor (if you are running Check Point FP2) or Check Point SmartDashboard (if you are running Check Point FP3) to control what data is logged by the firewalls to the Check Point Log Server.

For more information, see your Check Point documentation.

Configuring Check Point policies

There are two steps to configuring Check Point policies for use in logging events to the Symantec Event Collector for Check Point:

- In the SESA Console, determine the data that you want to see in your SESA reports.
- In Check Point, configure policies that generate that data.

For example, if you want to see a pie chart of traffic by service, configure Check Point to log connections using the services you are interested in. To see a graph depicting denied connections, configure Check Point to log denied connections. Remember that the statistics involved (numbers, percentages, frequencies, and so forth) are based on what is actually logged.

To determine what you want Check Point to log

- 1 In the SESA Console, on the Events view tab, in the left pane, expand the **Firewall Events Family** folder.
See [“Viewing reports installed for the Symantec Event Collector for Check Point”](#) on page 42.
- 2 Click on the report you want to view.
- 3 In the right pane, if the report displayed is a graph or pie chart, click on a section of the graph to display a table of events on which it is based.
- 4 In the table, view the column headings to see what data is represented by the report.

To create Check Point policies

- 1 Do one of the following:
 - If you are using Check Point VPN-1/FireWall-1 FP2, open the Check Point Policy Editor.
 - If you are using Check Point VPN-1/FireWall-1 FP3, open the Check Point SmartDashboard.
- 2 For each rule, decide whether and how you want to enable tracking:
 - For rules that control connections that you do not want to log, leave tracking turned off.
 - To log statistical information so that it appears in Firewall Event Family reports, set Track to Account.
 - To log connection events so that they appear in the Check Point specific reports and the Firewall Event Family reports, set Track to Log.
- 3 To log the accessing of individual files through FTP, or individual Web pages through HTTP or HTTPS, configure a rule that uses a “Service with Resource.”
- 4 To draw special attention to some particular type of event, configure it to be logged as a Check Point alert.

When the Check Point software issues a log message as an alert, the Symantec Event Collector for Check Point prioritizes it as a warning and includes the alert type in the “Alert Type” field.

In the SESA Console, you can filter reports that are based on these events.
- 5 Additional logging options are available for various features in the Log and Alert tab of the Global Properties window.

Customizing the SESA Agent configuration

The SESA Agent uses default logging parameters that are appropriate for most event collection circumstances. However, in extreme situations the Symantec Event Collector for Check Point can overrun the SESA Agent’s ability to flush event to the SESA Manager.

The recommendations in this section provide for maximum event throughput from the Symantec Event Collector for Check Point to the SESA Manager. They allow the SESA Agent to queue up as many firewall events as possible.

You adjust SESA Agent parameters from the Configuration view tab of the SESA Console. For more information, see the section on configuring products in the *Symantec Enterprise Security Architecture Administrators Guide*.

For the best performance and reliability, use the Configurations view tab of the SESA Console to change the configuration parameters for the SESA Agent as described in [Table 3-2](#).

To customize the SESA Agent configuration

- 1 On the Configurations view tab, in the left pane, expand the SESA folder.
- 2 Expand SESA Agent Configuration.
- 3 On the Logging tab, change the parameters to the settings described in [Table 3-2](#).
- 4 When you finish editing the configuration, select one of the following:
 - Apply: Save your changes and continue editing.
 - Reset: Cancel all of the changes that you have made on all of the tabs and reset the values to those that existed when you started editing.
- 5 When you are prompted to distribute the changes, select one of the following:
 - Yes: Immediately informs computers that are associated with the configuration of the changes. The computers receive a message that a new configuration is waiting.
 - No: Inform computers of the changes at a later time, or the computers will pick up changes at the next scheduled configuration update interval.When you distribute a configuration, the software of the target systems will retrieve their new configuration when the config poll time is reached.

Note: For information on all SESA Agent parameters and settings, see the chapter on configuring products in the *Symantec Enterprise Security Architecture Administrators Guide*.

Table 3-2 Recommended SESA Agent settings

Parameter	Recommended Setting	Description
Maximum queue size	9999 kb	When an application’s queue reaches this size any future log requests will be refused

Table 3-2 Recommended SESA Agent settings (Continued)

Parameter	Recommended Setting	Description
App flush size	999 kb	Agent outbound data is sent to the SESA Manager whenever one of the three triggers is tripped. Note: This only applies to batch events. Direct events are always sent as soon as possible. By default, the SESA Agent waits 5 minutes to forward events unless the App flush count is exceeded. Reducing the App flush time limits how many events queue up or how long before they are sent to the SESA Manager.
App flush count	1000	
App flush time	30 seconds	
App spool size	1000 kb	The size in kilobytes of the Symantec Event Collector for Check Point queue that the SESA Agent will hold in memory when not able to send the normal queue to the SESA Manager. If the queue exceeds this size and it still needs to grow, the queue will be written to disk.

Index

A

- Add/Remove Programs, Symantec Event Collector for Check Point 39
- agent.settings file 37
- alerts
 - affect on log messages 16
 - configuring in Check Point policies 45
- Application Library, SESA Agent 14
- Application Log, verifying Symantec Event Collector for Check Point operation 39

C

- CD contents, Symantec Event Collector for Check Point 18
- Check Point
 - events processed 15
 - mapping of events to SESA 15
- Check Point Log Server
 - allowing traffic to SESA Manager 24
 - configuring for Symantec Event Collector for Check Point 44
 - configuring the LEA port 25
 - connectivity to SESA Manager 23
 - installing SESA Agent 30, 33
 - installing Symantec Event Collector for Check Point 33
 - system requirements 24
- Check Point policies
 - configuring alerts 45
 - configuring services 45
 - enabling tracking 45
- Check Point Policy Editor 45
- Check Point SmartDashboard 45
- Configuration view tab, SESA Console 45
- configurations
 - distributing changes 46

- connectivity
 - between Check Point Log Server and SESA Manager 23
 - testing 23
- custom reports, creating 43

D

- data
 - processing, Symantec Event Collector for Check Point 14
 - retrieval, Symantec Event Collector for Check Point 14
- distribute
 - from configuration 46

E

- Event Collector
 - See Symantec Event Collector for Check Point

F

- Firewall Event Family
 - viewing in SESA Console 35

I

- installing
 - Java Runtime Library 29
 - planning 20
 - SESA Agent 30, 33
 - Symantec Event Collector for Check 33
 - Symantec Event Manager for Firewall 30
 - troubleshooting 37
 - verification 35

J

- JRE, installing 29

L

- LEA
 - configuring port for Symantec Event Collector for Check Point 25
 - description 14
- Log Export API *See* LEA
- log file
 - Symantec Event Collector for Check Point 36
 - viewing for SESA Agent 36
- log messages
 - alert field 16
 - severity 16
- logging parameters, configuring for SESA Agent 45

M

- message queue limits, SESA Agent 15

R

- removing. *See* uninstalling
- reports
 - customizing 43
 - viewing in SESA Console 35, 42

S

- services
 - configuring in Check Point policies 45
- SESA Agent
 - Application Library 14
 - configuring logging parameters 45
 - description 14
 - installing 30, 33
 - message queue limits 15
 - viewing agent log 36
- SESA Console
 - Configuration view tab 45
 - logging on 35
 - viewing Firewall Event Family 35
 - viewing Symantec Event Collector for Check Point logs 35

- SESA DataStore, system requirements 26
- SESA integration components, installing for Symantec Event Collector for Check Point 26
- SESA Manager
 - connectivity to Check Point Log Server 23
 - installing SESA integration components 26
 - system requirements 23
 - verifying IP address and port 37
- severity, log messages 16
- Symantec Event Collector for Check Point
 - CD contents 18
 - components installed 11, 22
 - data processing 14
 - data retrieval 14
 - description 10
 - events processed 15
 - installation, planning 20
 - installing 33
 - installing SESA integration components 26
 - log, examining 36
 - mapping of Check Point Events 15
 - system requirements 22
 - topology 13
 - uninstalling 39
 - verifying installation 35
 - verifying operation 38
 - viewing in SESA Console 35
- Symantec Event Manager for Firewall
 - installing 30
 - uninstalling 40
- system requirements
 - Check Point Log Server 24
 - SESA DataStore 26
 - SESA Manager 23
 - Symantec Event Collector for Check Point 22

T

- tracking, enabling for Check Point policies 45
- troubleshooting installations 37

U

uninstalling

Symantec Event Collector for Check Point 39

Symantec Event Manager for Firewall 40

V

verifying

SESA operation 35

Symantec Event Collector for Check Point
installation 35